

The broadcast classical-quantum capacity region of a two-phase bidirectional relaying channel

Holger Boche · Minglai Cai · Christian Deppe

the date of receipt and acceptance should be inserted later

Abstract We studied a three-node quantum network that enables bidirectional communication between two nodes with a half-duplex relay node for transmitting classical messages. A decode-and-forward protocol is used to perform the communication in two phases. In the first phase, the messages of two nodes are transmitted to the relay node. The capacity of the first phase is well-known by previous works. In the second phase, the relay node broadcasts a re-encoded composition to the two nodes. We determine the capacity region of the broadcast phase. To the best of our knowledge, this is the first paper analyzing quantum bidirectional relay networks.

Keywords Quantum information theory; Quantum network; Quantum relay channel; Quantum broadcast channel

1 Introduction

The study of quantum channel networks has become more and more important in the last few years.

Some of the first applications of this will be secret key transmission/generation and transmitting of secure messages over quantum networks. The capacities for secret key transmission/generation and the secrecy capacities for message transmission have been determined in [14] and [11].

For these applications, the transmitters have to solve two main problems. First, the message (a secret key or a secure message) has to be encoded in such a way that it can be decoded correctly by the legal receiver. Second, the message has to be encoded such that the wiretapper's knowledge of the transmitted classical message can be kept arbitrarily small.

Lehrstuhl für Theoretische Informationstechnik,
Technische Universität München,
Munich, Germany
E-mail: {boche, minglai.cai, christian.deppe}@tum.de

Transmission of secret keys and secure messages over long distances is an essential requirement for those applications. Thus, in our paper, we consider the problem how to ensure that the legal receivers are able to reproduce the original messages. This is a necessary condition for reliable secret key transmissions/generations and transmitting of secure messages over quantum networks.

The problem of long-distance transmissions of quantum information is one of the biggest problems in the realization of quantum networks. The sending of photons in optical fibers is presently limited by 200 km because of losses in the optical-fiber channel due to absorption on the way. One solution to solve this problem is the development of quantum repeaters (cf. [10] and [1]). Unfortunately, the practical realization of this component is not given until now. The researchers already built quantum repeaters in their laboratories, but until now it is not possible to extend the limit of 200 km.

In this paper, we use a relay instead of a quantum repeater. The advantage of this protocol is that it is realizable and enables quantum communication between two parties over the double length of the distance for sending photons in optical fibers. This protocol can also be used for free space optical communications between satellites. The communications in several classical practical applications such as satellite communication and cellular communication are modeled with channels with relay nodes. Channel networks with relay nodes have been studied extensively in the context of classical information theory (cf. [24] and [13]). The study of quantum channels with relay nodes has just recently begun (cf. [36]).

We analyze a quantum channel network model which was introduced for classical channel networks in [33]. It is called the two-phase bidirectional relaying channel (Figure 1). In this model we consider a three-node quantum network with two message sets M_1 and M_2 , which is called a two-user bidirectional quantum channel. The message $m_2 \in M_2$ is located at node 1, and the message $m_1 \in M_1$ is located at node 2, respectively, while a relay node enables the bidirectional communication between these nodes. We assume that the relay node cannot transmit and receive data at the same time. This is usually called a half-duplex relay. This assumption is reasonable for practical components in communication systems in general.

Our goal is that after the transmission the message $m_2 \in M_2$ is known at node 2 and the message $m_1 \in M_1$ is known at node 1, respectively. We simplify the problem by assuming an a priori separation of the communication into two phases.

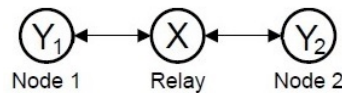


Fig. 1: Two-phase bidirectional relaying channels

There exist several strategies which are usually classified by the process at the relay node, namely the entanglement swapping-and-forward strategy (cf. [23]) and the decode-and-forward strategy. We consider a two-phase decode-and-forward protocol. The relay node's task is to decode the messages that it receives in the first phase and to forward the information to its destinations in the second phase. This basically means that in the first phase the relay measures and decodes and that in the second phase the relay prepares and encodes. The disadvantage of this strategy is that the coherence is destroyed. The advantage of this strategy is that in the second phase each receiver can use its own message from the first phase as side information to gather a higher capacity.

The goal of the communication is the transmission of classical signals, between two partners. The problem of the optimal transmission of these classical signals can be divided into two parts:

1. Quantum modulation (i.e., choosing an optimal set of possible input states which will be the input alphabet. This is equivalent to consider a special classical-quantum channel, i.e., a quantum channel depending on the set of chosen input states whose sender's inputs are classical variables.)
2. Optimal coding for the classical-quantum channel.

We also consider this problem because the model of classical-quantum channels is a very important tool for understanding the capacity formulas for quantum channels. The capacity of classical-quantum channels has been determined in [20], [21], and [41]. It turns out that classical-quantum channels are not only of theoretical interest, but as well as of technical interest, too; for instance, a code for a classical-quantum channel can be used for entanglement generation (cf. [14]). Furthermore, new phenomenons such as super-additivity and super-activation appear for carrying classical information through a quantum channel (cf. [8]).

We would like to point out that the three-node bidirectional relay network is an extremely advantageous tool in the relay network theory. The model of classical three-node bidirectional relay network has been extended to more complex models such as MIMO channels ([30], [15], [37], [32]), Gaussian channels ([37]), polar codes ([5]), and cross-layer designs ([27], [28], [29]). In view of these previous works on the classical bidirectional relay network, our further tasks will be to analyze these models for quantum networks (cf. [22], [17], and [43]).

For classical models, the authors of [33] use results from coding theory for degraded broadcast channel (cf. [6]). One of our major challenges in this paper is that there are no equivalent tools in the quantum information theory yet. Thus, we can only establish the capacity region with average errors, but not the capacity region with maximal errors as in the classical case (cf. Remark 2). It still reminds open how the capacity region with maximal errors can be established.

Recent research has been done toward security for classical bidirectional relay networks (cf. [39] and [5]). It is a promising task to find similar results for quantum networks.

Another important basic feature for classical bidirectional relay networks is the channel uncertainty ([38], [31]). The capacity for quantum channels with uncertainty has been determined in [4], [7], and [8].

The design of communication protocols for quantum networks is a challenging task. For the design of efficient protocols, it is important to incorporate side information into the coding schemes. In this paper, we considered the case where both receivers have side information about the messages. [9] considered recently the case where the transmitter has side information about the channel state. This corresponds to the classical “writing on dirty paper” coding. This coding strategy plays an important role in modern communication systems. It is an interesting research topic to develop on the basis of [9] and the bidirectional relaying protocol of this paper for more complicated quantum networks.

The study of relay channels in the quantum scenario is novel. We hope our results may raise interests in further analysis.

2 Basic definitions

2.1 A two-phase protocol

By the separation of the communication, we have a multiple-access phase, where node 1 and node 2 transmit messages m_2 and m_1 to the relay node, and a broadcast phase, where the relay forwards the messages to node 2 and node 1, respectively. We look at the two phases separately.

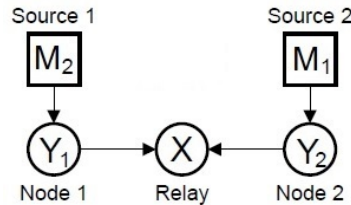


Fig. 2: The multiple access phase

In the multiple-access phase, we have a classical-quantum multiple-access channel. The multiple-access channel is a channel such that two (or more) senders send information to a common receiver via this channel. The optimal coding strategies and capacity regions for classical multiple-access channels

have been given in [3] and [25]. The optimal coding strategies and capacity regions for multiple-access quantum channels have been given in [45] and [46].

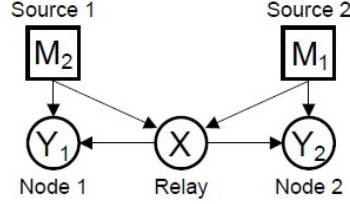


Fig. 3: The broadcast phase

In the broadcast phase, we have a broadcast quantum channel. In a broadcast channel, one single sender sends information to two (or more) receivers. The optimal coding strategies and capacity regions for classical broadcast channels have been given in [26], [6], and [18]. An optimal coding strategy and a capacity region for broadcast quantum channels have been given in [35].

For the broadcast phase, we assume that the relay node has successfully decoded the messages m_1 and m_2 in the multiple-access phase. Of course, the message m_2 is also known at node 1 and the message m_1 is also known at node 2.

The goal of the relay node is to broadcast a message to node 1 and node 2 which allows both nodes to recover the unknown source. This means that node 1 wants to recover message m_1 and that node 2 wants to recover message m_2 .

2.2 Notations and communication scenarios

For finite-dimensional complex Hilbert spaces G and G' , a quantum channel $N: \mathcal{S}(G) \rightarrow \mathcal{S}(G')$, $\mathcal{S}(G) \ni \rho \rightarrow N(\rho) \in \mathcal{S}(G')$ is represented by a completely positive trace-preserving map that accepts input quantum states in $\mathcal{S}(G)$ and produces output quantum states in $\mathcal{S}(G')$. Here, $\mathcal{S}(G)$ stands for the space of density operators on the space G .

If the sender wants to transmit a classical message of a finite set A to the receiver using a quantum channel N , his encoding procedure will include a classical-to-quantum encoder to prepare a quantum message state $\rho \in \mathcal{S}(G)$ suitable as an input for the channel. If the sender's encoding is restricted to transmit an indexed finite set of quantum states $\{\rho_x : x \in A\} \subset \mathcal{S}(G)$, then we can consider the choice of the signal quantum states ρ_x as a component of the channel. Thus, we obtain a channel $\sigma_x := N(\rho_x)$ with classical inputs $x \in A$

and quantum outputs, which we call a classical-quantum channel. This is a map $\mathbf{N}: A \rightarrow \mathcal{S}(G')$, $A \ni x \rightarrow \mathbf{N}(x) \in \mathcal{S}(G')$ which is represented by the set of $|A|$ possible output quantum states $\{\sigma_x = \mathbf{N}(x) := N(\rho_x) : x \in A\} \subset \mathcal{S}(G')$, meaning that each classical input of $x \in A$ leads to a distinct quantum output $\sigma_x \in \mathcal{S}(G')$. In view of this, we have the following definition.

Let H be a finite-dimensional complex Hilbert space. A classical-quantum channel is a map $N: A \rightarrow \mathcal{S}(H)$, $A \ni a \rightarrow N(a) \in \mathcal{S}(H)$.

For a probability distribution P on a finite set A and a positive constant δ , we denote the set of typical sequences by

$$\mathcal{T}_{P,\delta}^n := \left\{ x^n \in A^n : \left| \frac{1}{n} \langle x^n | a \rangle - P(a) \right| \leq \frac{\delta}{|A|} \right\},$$

where $\langle x^n | a \rangle$ is the number of occurrences of the symbol a in the sequence x^n .

Let $n \in \mathbb{N}$, we define $A^n := \{(a_1, \dots, a_n) : a_i \in A \forall i \in \{1, \dots, n\}\}$. The space which the vectors $\{v_1 \otimes \dots \otimes v_n : v_i \in H \forall i \in \{1, \dots, n\}\}$ span is defined by $H^{\otimes n}$. We also write a^n for the elements of A^n .

Associated with a classical quantum channel, $N: A \rightarrow \mathcal{S}(H)$ is the channel map on the n -block $N^{\otimes n}: A^n \rightarrow \mathcal{S}(H^{\otimes n})$ such that for $a^n = (a_1, \dots, a_n) \in A^n$. We have $N^{\otimes n}(a^n) = N(a_1) \otimes \dots \otimes N(a_n)$.

For a quantum state $\rho \in \mathcal{S}(G)$, we denote the von Neumann entropy of ρ by

$$S(\rho) = -\text{tr}(\rho \log \rho).$$

Let $\mathbf{V}: A \rightarrow \mathcal{S}(G)$ be a classical-quantum channel. For $P \in P(A)$ the conditional entropy of the channel for \mathbf{V} with input distribution P is denoted by

$$S(\mathbf{V}|P) := \sum_{x \in A} P(x) S(\mathbf{V}(x)).$$

Remark 1 The following definition is a more general definition of the conditional entropy in quantum information theory. Let \mathfrak{P} and \mathfrak{Q} be quantum systems. We denote the Hilbert space of \mathfrak{P} and \mathfrak{Q} by $G^{\mathfrak{P}}$ and $G^{\mathfrak{Q}}$, respectively. Let $\phi^{\mathfrak{P}\mathfrak{Q}}$ be a bipartite quantum state in $\mathcal{S}(G^{\mathfrak{P}\mathfrak{Q}})$. We denote $S(\mathfrak{P} | \mathfrak{Q})_\rho := S(\phi^{\mathfrak{P}\mathfrak{Q}}) - S(\phi^{\mathfrak{Q}})$. Here $\phi^{\mathfrak{Q}} = \text{tr}_{\mathfrak{P}}(\phi^{\mathfrak{P}\mathfrak{Q}})$.

Let $\Phi := \{\rho_x : x \in A\}$ be a set of quantum states labeled by elements of A . For a probability distribution P on A the Holevo χ quantity is defined as

$$\chi(P; \Phi) := S\left(\sum_{x \in A} P(x) \rho_x\right) - \sum_{x \in A} P(x) S(\rho_x).$$

We denote the identity operator on a space G by id_G .

A collection of positive semi-definite operators $\{M_i : i\}$ on G is called a positive operator valued measure, or POVM, if it is a partition of the identity, i.e., $\sum_i M_i = \text{id}_G$.

2.3 Code concepts

A two-user multiple-access quantum channel $N_{BC-A} : H^{BC} \rightarrow H^A$ has two senders B and C , and a single receiver A . It is defined as a map $N : H^{BC} \rightarrow H^A$.

An $(n, J_n^{(1)}, J_n^{(2)})$ code carrying classical information for a two-user quantum multiple access channel $N_{BC-A} : H^{BC} \rightarrow H^A$ consists of an ensemble of quantum states $\{w(m_1) : m_1 = 1, \dots, J_n^{(1)}\} \subset \mathcal{S}(H^{B^{\otimes n}})$, quantum states $\{v(m_2) : m_2 = 1, \dots, J_n^{(2)}\} \subset \mathcal{S}(H^{C^{\otimes n}})$, and a POVM $\left\{D_{m_1, m_2} : m_1 \in \{1, \dots, J_n^{(1)}\}, m_2 \in \{1, \dots, J_n^{(2)}\}\right\}$ on $H^{A^{\otimes n}}$.

A pair of nonnegative numbers (R_1, R_2) is an achievable rate pair with classical inputs for the quantum multiple-access channel $N_{BC-A} : H^{BC} \rightarrow H^A$ with average error if for every positive ε , δ , and a sufficiently large n there is an $(n, J_n^{(1)}, J_n^{(2)})$ code carrying classical information $(\{w(m_1) : m_1 = 1, \dots, J_n^{(1)}\}, \{v(m_2) : m_2 = 1, \dots, J_n^{(2)}\}, \{D_{m_1, m_2} : m_1 \in \{1, \dots, J_n^{(1)}\}, m_2 \in \{1, \dots, J_n^{(2)}\}\})$ such that $\frac{1}{n} \log J_n^{(1)} \geq R_1 - \delta$, $\frac{1}{n} \log J_n^{(2)} \geq R_2 - \delta$ and

$$\frac{1}{J_n^{(1)} J_n^{(2)}} \sum_{m_1=1}^{J_n^{(1)}} \sum_{m_2=1}^{J_n^{(2)}} \text{tr} \left((\text{id}_{H^{A^{\otimes n}}} - D_{m_1, m_2}) N_{BC-A}^{\otimes n} (w(m_1), v(m_2)) \right) \leq \varepsilon. \quad (1)$$

The two-user broadcast quantum channel $N_{A-BC} : H^A \rightarrow H^{BC}$ is a quantum channel from a single sender A to two independent receivers B and C . The quantum channel W_1 from A to B is obtained by tracing out C from the channel map, i.e., $W_1 = N_{A-B} : H^A \rightarrow H^B$, which is the quantum channel from A to B , is defined as $W_1(\sigma) = \text{tr}_C(N_{A-BC}(\sigma))$. Furthermore, $W_2 = N_{A-C} : H^A \rightarrow H^C$, which is the quantum channel from A to C , is defined as $W_2(\sigma) = \text{tr}_B(N_{A-BC}(\sigma))$.

An $(n, J_n^{(1)}, J_n^{(2)})$ code carrying classical information for a two-user broadcast quantum channel $N_{A-BC} : H^A \rightarrow H^{BC}$ consists of an ensemble $\{w((m_1, m_2)) : m_1 = 1, \dots, J_n^{(1)}, m_2 = 1, \dots, J_n^{(2)}\} \subset \mathcal{S}(H^{A^{\otimes n}})$, a POVM $\left\{D_{m_1}^{(1)} : m_1 \in \{1, \dots, J_n^{(1)}\}\right\}$ on $H^{B^{\otimes n}}$, and a POVM $\left\{D_{m_2}^{(2)} : m_2 \in \{1, \dots, J_n^{(2)}\}\right\}$ on $H^{C^{\otimes n}}$.

A pair of nonnegative numbers (R_1, R_2) is an achievable rate pair with a classical input for the two-user broadcast quantum channel $N_{A-BC} : H^A \rightarrow H^{BC}$ with average error if for every positive ε , δ , and a sufficiently large n there is an $(n, J_n^{(1)}, J_n^{(2)})$ code carrying classical information $(\{w_t(j) : j\}, \{D_j : j\})$ such that $\frac{1}{n} \log J_n^{(1)} \geq R_1 - \delta$, $\frac{1}{n} \log J_n^{(2)} \geq R_2 - \delta$, for every $m_2 \in M_2$

$$\frac{1}{J_n^{(1)}} \sum_{j=1}^{J_n^{(1)}} \text{tr} \left((\text{id}_{H^{B^{\otimes n}}} - D_{m_1}^{(1)}) W_1^{\otimes n} (w((m_1, m_2))) \right) \leq \varepsilon, \quad (2)$$

and for every $m_1 \in M_1$

$$\frac{1}{J_n^{(2)}} \sum_{j=1}^{J_n^{(2)}} \text{tr} \left((\text{id}_{H^{C \otimes n}} - D_{m_2}^{(1)}) W_2^{\otimes n} (w((m_1, m_2))) \right) \leq \varepsilon, \quad (3)$$

where $W_1 = N_{A-B}$ and $W_2 = N_{A-C}$.

The capacity regions of multiple-access quantum channels and broadcast quantum channels are convex by the time-sharing principle: Let (R_1, R_2) and (R'_1, R'_2) be rate tuples of m and n block codes, respectively, with error probabilities ϵ_1 and ϵ_2 , respectively. We get an $(m+n)$ block code with error probability at most $\epsilon_1 + \epsilon_2$ and with rates $\left(\frac{m}{m+n} R_1 + \frac{n}{m+n} R'_1, \frac{m}{m+n} R_2 + \frac{n}{m+n} R'_2 \right)$ by concatenating the code words to $(m+n)$ blocks and tensoring the corresponding decoding observables.

3 The classical-quantum capacity region of the bidirectional relaying quantum channel

For the multiple-access phase, the optimal coding strategy is well known from [45], where the following lemma for the classical-quantum rate region of multiple-access quantum channels was given.

Lemma 1 *Let $N_{Y_2 Y_1 - X}$ be a two-user multiple-access quantum channel. Let H^{Y_1} be the Hilbert space whose unit vectors correspond to the pure states of node 1's quantum system, H^{Y_2} be the Hilbert space whose unit vectors correspond to the pure states of node 2's quantum system, and H^X be the Hilbert space whose unit vectors correspond to the pure states of the relay node's quantum system.*

We assume node 1's encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $Y_1 \subset H^{Y_1}$.

We assume node 2's encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $Y_2 \subset H^{Y_2}$.

The classical-quantum capacity region of the multiple-access quantum channel $N_{Y_2 Y_1 - X}$ with average error is given by the set of all rate pairs (R_2, R_1) , satisfying

$$R_2 \leq \chi(Q_1; \sigma^X), \quad (4)$$

$$R_1 \leq \chi(Q_2; \sigma^X), \quad (5)$$

and

$$R_2 + R_1 \leq \chi(Q_{1,2}; \sigma^X) \quad (6)$$

for any joint probability distribution $Q_{1,2}$ on $Y_1 \times Y_2$. Here, Q_1 is the marginal probability distribution of $Q_{1,2}$ on Y_1 , Q_2 is the marginal probability distribution of $Q_{1,2}$ on Y_2 , and σ^X is the resulting quantum state at the outcome of the relay node.

Thus, if n is sufficiently large and if for M_1 and M_2 it holds

$$|M_2| \leq \lfloor 2^{n(\chi(Q_1; \sigma^X) - \epsilon)} \rfloor ,$$

$$|M_1| \leq \lfloor 2^{n(\chi(Q_2; \sigma^X) - \epsilon)} \rfloor ,$$

and

$$|M_2| + |M_1| \leq \lfloor 2^{n(\chi(Q_{1,2}; \sigma^X) - \epsilon)} \rfloor$$

for some positive ϵ , we can assume that the relay node has successfully decoded the messages $m_1 \in M_1$ and $m_2 \in M_2$.

Note that the author of [45], using block codes and showing a weak converse, is able to give (4), (5), and (6) in single letter formula. Please see [9] for more discussions on the value of multiletter formulas for quantum communication networks.

For the broadcast phase, since each node has perfect knowledge about the message intended for the other, one can use this knowledge as a support for the choice of the decoding strategy to decode the message intended for itself. In view of these facts, we have the following Theorem 1.

Theorem 1 *Let N be a two-user bidirectional quantum channel. Let H^{Y_1} be the Hilbert space whose unit vectors correspond to the pure states of node 1's quantum system, H^{Y_2} be the Hilbert space whose unit vectors correspond to the pure states of node 2's quantum system, and H^X be the Hilbert space whose unit vectors correspond to the pure states of the relay node's quantum system. Let $N_{X-Y_1Y_2}$ be the broadcast quantum channel in the broadcast phase.*

We assume that the relay node's encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $\{\phi_x : x \in X\} \subset H^X$.

For all probability distribution P on X , the capacity region of the bidirectional broadcast quantum channel $N_{X-Y_1Y_2}$ during the broadcast phase for transmitting classical information with average error is given by the set of all rate pairs (R_1, R_2) , satisfying

$$R_1 \leq \limsup_{n \rightarrow \infty} \frac{1}{n} \chi(P^n; \sigma^{Y_1 \otimes n}) \quad (7)$$

and

$$R_2 \leq \limsup_{n \rightarrow \infty} \frac{1}{n} \chi(P^n; \sigma^{Y_2 \otimes n}) . \quad (8)$$

Here, σ^{Y_1} is the resulting quantum state at the outcome of node 1, while σ^{Y_2} is the resulting quantum state at the outcome of node 2.

Proof It is easy to verify that every achievable rate pair cannot exceed (7) and (8). R_1 cannot exceed $\limsup_{n \rightarrow \infty} \frac{1}{n} \chi(P^n; \sigma^{Y_1 \otimes n})$, even if the relay node only sends a message to node 1 without sending any message to node 2 (cf. [21]). For the same reason, R_2 cannot exceed $\limsup_{n \rightarrow \infty} \frac{1}{n} \chi(P^n; \sigma^{Y_2 \otimes n})$ either. Now we will prove the achievability of the extremal point of the rate region given by

(7) and (8), since then every rate pair in the rate region is achievable by the time-sharing principle.

At first, we present some tools which that were used for our proof:

Let H be a Hilbert space. For $\rho \in \mathcal{S}(H)$ and $\alpha > 0$ there exists an orthogonal subspace projector $\Pi_{\rho,\alpha}$ commuting with $\rho^{\otimes n}$ and satisfying

$$\mathrm{tr}(\rho^{\otimes n} \Pi_{\rho,\alpha}) \geq 1 - \frac{d}{4n\alpha^2}, \quad (9)$$

$$\mathrm{tr}(\Pi_{\rho,\alpha}) \leq 2^{nS(\rho) + Kd\alpha\sqrt{n}}, \quad (10)$$

$$\Pi_{\rho,\alpha} \cdot \rho^{\otimes n} \cdot \Pi_{\rho,\alpha} \leq 2^{-nS(\rho) + Kd\alpha\sqrt{n}} \Pi_{\rho,\alpha}, \quad (11)$$

where $d := \dim H$ and K is a positive constant (cf. [42]).

Let A be a finite set and let $\mathbf{V} : A \rightarrow \mathcal{S}(H)$ be a classical-quantum channel. For a probability distribution P on A , $\alpha > 0$, and $x^n \in \mathcal{T}_P^n$ there exists an orthogonal subspace projector $\Pi_{\mathbf{V},\alpha}(x^n)$ commuting with $\mathbf{V}_{x^n}^{\otimes n}$ and satisfying

$$\mathrm{tr}(\mathbf{V}^{\otimes n}(x^n) \Pi_{\mathbf{V},\alpha}(x^n)) \geq 1 - \frac{ad}{4n\alpha^2}, \quad (12)$$

$$\mathrm{tr}(\Pi_{\mathbf{V},\alpha}(x^n)) \leq 2^{nS(\mathbf{V}|P) + Kd\alpha\sqrt{n}}, \quad (13)$$

$$\begin{aligned} & \Pi_{\mathbf{V},\alpha}(x^n) \cdot \mathbf{V}^{\otimes n}(x^n) \cdot \Pi_{\mathbf{V},\alpha}(x^n) \\ & \leq 2^{-nS(\mathbf{V}|P) + Kd\alpha\sqrt{n}} \Pi_{\mathbf{V},\alpha}(x^n), \end{aligned} \quad (14)$$

where $a := \#A$ and K is a positive constant (cf. [42]).

Let $\mathbf{V} : A \rightarrow \mathcal{S}(H)$ be a classical-quantum channel. Then, every probability distribution P on A defines a quantum state $P\mathbf{V}$ on $\mathcal{S}(H)$, which is the resulting quantum state at the output of \mathbf{V} when the input is sent according to P . Thus, for $\alpha' > 0$ we can define an orthogonal subspace projector $\Pi_{P\mathbf{V},\alpha'\sqrt{a}}$ which fulfills (9), (10), and (11) (here, we set $\rho = P\mathbf{V}$ and $\alpha = \alpha'\sqrt{a}$). Furthermore, for $\Pi_{P\mathbf{V},\alpha'\sqrt{a}}$, we have the following inequality

$$\mathrm{tr}(\mathbf{V}^{\otimes n}(x^n) \cdot \Pi_{P\mathbf{V},\alpha'\sqrt{a}}) \geq 1 - \frac{ad}{4n\alpha^2}, \quad (15)$$

where K is a positive constant (cf. [42]).

Lemma 2 (Measurement on Approximately Close States, cf. [42])

Let σ and ρ be two quantum states, and let Π be a positive operator such that $\Pi \leq \mathrm{id}$; then,

$$\mathrm{tr}(\Pi\sigma) \geq \mathrm{tr}(\Pi\rho) - \|\sigma - \rho\|_1.$$

Lemma 3 (Tender Operator, cf. [44] and [34]) Let ρ be a quantum state.

Let X be a positive operator such that $X \leq \mathrm{id}$ and $1 - \mathrm{tr}(\rho X) \leq \lambda \leq 1$; then,

$$\|\rho - \sqrt{X}\rho\sqrt{X}\| \leq \sqrt{8\lambda}. \quad (16)$$

Lemma 4 (Hayashi-Nagaoka Operator Inequality, cf. [19]) *For any positive operators S and T such that $S \leq \text{id}$ we have*

$$\text{id} - (S + T)^{-\frac{1}{2}} S (S + T)^{-\frac{1}{2}} \leq (\text{id} - S) + 4T . \quad (17)$$

The random encoding technique:

We denote $W_1 = N_{X-Y_1}$ and $W_2 = N_{X-Y_2}$. For any positive ϵ let M'_1 be a message set such that $|M'_1| \leq 2^{n(\chi(P; \sigma^{Y_1}) - 2\epsilon)}$, and let M'_2 be a message set such that $|M'_2| \leq 2^{n(\chi(P; \sigma^{Y_2}) - 2\epsilon)}$. We generate $|M'_1||M'_2|$ independent random variables

$$\{X^n(m_1, m_2) : m_1 \in M'_1, m_2 \in M'_2\}$$

taking values in \mathcal{T}_P^n i.i.d. according to the product distribution $P(x^n) = \prod_{i=1}^n P(x_i)$.

For all $x^n \in X^n$ we define $\Pi_{PW_1, \alpha\sqrt{a}}$ on $H^{Y_1 \otimes n}$, $\Pi_{PW_2, \alpha\sqrt{a}}$ on $H^{Y_2 \otimes n}$, $\Pi_{W_1^{\otimes n}(x^n), \alpha}$ on $H^{Y_1 \otimes n}$, and $\Pi_{W_2^{\otimes n}(x^n), \alpha}$ on $H^{Y_2 \otimes n}$ as in (12), (13), (14), and (15). Here, we set $P = P$, $\mathbf{V} = W_1$, and $= W_2$, respectively. α is some positive constant which we will choose later. We define

$$D'_{x^n(1)} := \Pi_{PW_1, \alpha\sqrt{a}} \Pi_{W_1^{\otimes n}(x^n), \alpha} \Pi_{PW_1, \alpha\sqrt{a}} ,$$

and

$$D'_{x^n(2)} := \Pi_{PW_2, \alpha\sqrt{a}} \Pi_{W_2^{\otimes n}(x^n), \alpha} \Pi_{PW_2, \alpha\sqrt{a}} .$$

Analysis of errors of the first kind:

We say an error of the first kind occurs if (m_1, m_2) has been send by the relay node, and either node 1 fails to decode m_1 or node 2 fails to decode m_2 .

For all $(m_1, m_2) \in M'_1 \times M'_2$ and any realization $x^n(m_1, m_2)$ of $X^n(m_1, m_2)$ we have

$$\begin{aligned} & \text{tr} \left(W_1^{\otimes n}(x^n(m_1, m_2)) D'_{x^n(1)} \right) \\ &= \text{tr} \left(W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{PW_1, \alpha\sqrt{a}} \Pi_{W_1^{\otimes n}(x^n(m_1, m_2)), \alpha} \Pi_{PW_1, \alpha\sqrt{a}} \right) \\ &= \text{tr} \left((\Pi_{PW_1, \alpha\sqrt{a}} W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{PW_1, \alpha\sqrt{a}}) \Pi_{W_1^{\otimes n}(x^n(m_1, m_2)), \alpha} \right) \\ &\geq \text{tr} \left(W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{W_1^{\otimes n}(x^n(m_1, m_2)), \alpha} \right) \\ &\quad - \left\| \Pi_{PW_1, \alpha\sqrt{a}} W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{PW_1, \alpha\sqrt{a}} - W_1^{\otimes n}(x^n(m_1, m_2)) \right\|_1 \\ &\geq 1 - \frac{d}{4n\alpha^2} \text{tr} \left(\Pi_{W^{\otimes n}(x^n(m_1, m_2)), \alpha} \right) \\ &\quad - \left\| \Pi_{PW_1, \alpha\sqrt{a}} W_1^{\otimes n}(x^n(m_1, m_2)) \Pi_{PW_1, \alpha\sqrt{a}} - W_1^{\otimes n}(x^n(m_1, m_2)) \right\|_1 \end{aligned}$$

$$\geq 1 - \frac{d}{4n\alpha^2} - \sqrt{8 \frac{ad}{4n\alpha^2}}. \quad (18)$$

The first inequality holds because of Lemma 2, the second inequality holds because of (12), and the third inequality holds because of Lemma 3 and (15).

Similarly, we have

$$\text{tr} \left(W_2^{\otimes n}(x^n(m_1, m_2)) D'_{x^n(m_1, m_2)}^{(2)} \right) \geq 1 - \frac{d}{4n\alpha^2} - \sqrt{8 \frac{ad}{4n\alpha^2}}. \quad (19)$$

Thus, the errors of the first kind go to zero if n is sufficiently large.

Analysis of errors of the second kind:

We define $\rho_2 := PW_2 = \sum_{x \in X} P(X)W_2(\phi_x)$; then, $\rho^{Y_2} = \rho_2$ if any realization of X^n is used to decode the input message. Let us fix $(m_1, m_2), (m'_1, m'_2) \in M'_1 \times M'_2$ such that $m_2 \neq m'_2$. Node 2 would make an error if (m_1, m_2) has been sent, but node 2's decoding results in the message m'_2 . We call it an error of the second kind. We now consider the expected value of the probability of this case, if we use the random encoder X^n to decode the input message. We have

$$\begin{aligned} & E \left[\text{tr} \left(W_2^{\otimes n}(X^n(m_1, m_2)) D'_{X^n(m_1, m'_2)}^{(2)} \right) \right] \\ &= \text{tr} \left[E \left(W_2^{\otimes n}(X^n(m_1, m_2)) \right) \cdot E \left(D'^{(2)}_{X^n(m_1, m'_2)} \right) \right] \\ &= \text{tr} \left[\rho_2^{\otimes n} E \left(D'^{(2)}_{X^n(m_1, m'_2)} \right) \right] \\ &= \text{tr} \left[\rho_2^{\otimes n} E \left(\Pi_{PW_2, \alpha\sqrt{a}} \Pi_{W_2^{\otimes n}(X^n(m_1, m'_2)), \alpha} \Pi_{PW_2, \alpha\sqrt{a}} \right) \right] \\ &= \text{tr} \left[E \left(\rho_2^{\otimes n} \Pi_{PW_2, \alpha\sqrt{a}} \Pi_{W_2^{\otimes n}(X^n(m_1, m'_2)), \alpha} \Pi_{PW_2, \alpha\sqrt{a}} \right) \right] \\ &= \text{tr} \left[E \left((\Pi_{PW_2, \alpha\sqrt{a}} \rho_2^{\otimes n} \Pi_{PW_2, \alpha\sqrt{a}}) \Pi_{W_2^{\otimes n}(X^n(m_1, m'_2)), \alpha} \right) \right] \\ &= \text{tr} \left[(\Pi_{PW_2, \alpha\sqrt{a}} \rho_2^{\otimes n} \Pi_{PW_2, \alpha\sqrt{a}}) E \left(\Pi_{W_2^{\otimes n}(X^n(m_1, m'_2)), \alpha} \right) \right] \\ &\leq 2^{-n[S(\rho_2) - \frac{1}{2}\epsilon]} \text{tr} \left[\Pi_{PW_2, \alpha\sqrt{a}} E \left(\Pi_{W_2^{\otimes n}(X^n(m_1, m'_2)), \alpha} \right) \right] \\ &\leq 2^{n[\sum_{x \in X} P(X)S(W_2(\phi_x)) - \frac{1}{2}\epsilon]} 2^{-n[S(\rho_2) - \frac{1}{2}\epsilon]} \text{tr} \left[\Pi_{PW_2, \alpha\sqrt{a}} \right] \\ &= 2^{-n[\sum_{x \in X} P(X)S(W_2(\phi_x)) - S(\sum_{x \in X} P(X)W_2(\phi_x)) - \epsilon]} \text{tr} \left[\Pi_{PW_2, \alpha\sqrt{a}} \right] \\ &= 2^{-n[\chi(P, \rho^{Y_2}) - \epsilon]} \text{tr} \left[\Pi_{PW_2, \alpha\sqrt{a}} \right] \\ &\leq 2^{-n[\chi(P, \rho^{Y_2}) - \epsilon]}. \end{aligned} \quad (20)$$

The first equality hold because $X^n(m_1, m_2)$ and $X^n(m_1, m'_2)$ are independent, the first inequality holds because of (11), and the second inequality holds because of (13).

Similarly, let us fix $(m'_1, m_2), (m_1, m_2) \in M'_1 \times M'_2$ such that $m_1 \neq m'_1$. Node 1 would make an error (of the second kind) if (m_1, m_2) has been sent, but node 1's decoding results in the message m'_1 . We now consider the expected value of the probability of this case if we use the random encoder X^n to decode the input message. We have

$$E \left[\text{tr} \left(W_1^{\otimes n}(X^n(m_1, m_2)) D'_{X^n(m_1, m'_2)^{(1)}} \right) \right] \leq 2^{-n[\chi(P, \rho^{Y_1}) - \epsilon]} . \quad (21)$$

Thus, the errors of the second kind go to zero if n is sufficiently large.

Definition of the code:

For all $(m_1, m_2) \in M'_1 \times M'_2$ we define

$$D_{X^n(m_1, m_2)}^{(1)} := \left(\sqrt{\sum_{m_1^* \in M'_1} D'^{(1)}_{X^n(m_1^*, m_2)}} \right)^{-1} D'^{(1)}_{X^n(m_1, m_2)} \left(\sqrt{\sum_{m_1^* \in M'_1} D'^{(1)}_{X^n(m_1^*, m_2)}} \right)^{-1} ,$$

and

$$D_{X^n(m_1, m_2)}^{(2)} := \left(\sqrt{\sum_{m_2^* \in M'_2} D'^{(2)}_{X^n(m_1, m_2^*)}} \right)^{-1} D'^{(2)}_{X^n(m_1, m_2)} \left(\sqrt{\sum_{m_2^* \in M'_2} D'^{(2)}_{X^n(m_1, m_2^*)}} \right)^{-1} ,$$

which depends on the random outcome of X^n . By construction, for any realization $\{x^n(m_1, m_2) : m_1 \in M'_1, m_2 \in M'_2\}$ of $\{X^n(m_1, m_2) : m_1 \in M'_1, m_2 \in M'_2\}$ we have for every $m_1 \in M'_1$,

$$\sum_{m_1 \in M'_1} D_{x^n(m_1, m_2)}^{(1)} \leq \text{id}_{H^{B \otimes n}} ,$$

and for every $m_2 \in M'_2$

$$\sum_{m_2 \in M'_2} D_{x^n(m_1, m_2)}^{(2)} \leq \text{id}_{H^{C \otimes n}} .$$

We combine (18) and (20), for all $(m_1, m_2) \in M'_1 \times M'_2$ we have

$$\begin{aligned} & E \left[\text{tr} \left(D_{X^n(m_1, m_2)}^{(1)} W_1^{\otimes n}(X^n(m_1, m_2)) \right) \right] \\ & \geq E \left[\text{tr} \left(D'^{(1)}_{X^n(m_1, m_2)} W_1^{\otimes n}(X^n(m_1, m_2)) \right) \right] \\ & \quad - 4E \left[\text{tr} \left(\sum_{m_1^* \neq m_1} D'^{(1)}_{X^n(m_1^*, m_2)} W_1^{\otimes n}(X^n(m_1, m_2)) \right) \right] \\ & \geq 1 - \frac{d}{4n\alpha^2} - \sqrt{8 \frac{ad}{4n\alpha^2}} \\ & \quad - 4E \left[\text{tr} \left(\sum_{m_1^* \neq m_1} D'^{(1)}_{X^n(m_1^*, m_2)} W_1^{\otimes n}(X^n(m_1, m_2)) \right) \right] \end{aligned}$$

$$\begin{aligned}
&\geq 1 - \frac{d}{4n\alpha^2} - \sqrt{8\frac{ad}{4n\alpha^2}} - 4|M'_1|2^{-n[\chi(P, \sigma^{Y_1}) - \epsilon]} \\
&\geq 1 - \frac{d}{4n\alpha^2} - \sqrt{8\frac{ad}{4n\alpha^2}} - 2^{-n\epsilon} .
\end{aligned} \tag{22}$$

The first inequity holds because of Lemma 4.

Similarly, if we combine (18) and (21), we have for all $(m_1, m_2) \in M'_1 \times M'_2$

$$E \left[\text{tr} \left(D_{X^n(m_1, m_2)}^{(2)} W_2^{\otimes n}(X^n(m_1, m_2)) \right) \right] \geq 1 - \frac{d}{4n\alpha^2} - \sqrt{8\frac{ad}{4n\alpha^2}} - 2^{-n\epsilon} . \tag{23}$$

Since (22) and (23) hold for all $(m_1, m_2) \in M'_1 \times M'_2$, for any positive ω , choosing a suitable α , if n is sufficiently large, we have

$$\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} E \left[\text{tr} \left(D_{X^n(m_1, m_2)}^{(1)} W_1^{\otimes n}(X^n(m_1, m_2)) \right) \right] \geq 1 - \omega$$

and

$$\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} E \left[\text{tr} \left(D_{X^n(m_1, m_2)}^{(2)} W_2^{\otimes n}(X^n(m_1, m_2)) \right) \right] \geq 1 - \omega .$$

By the law of large numbers, if n is sufficiently large, for any positive δ and γ , we have

$$p \left\{ \sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left(D_{X^n(m_1, m_2)}^{(1)} W_1^{\otimes n}(X^n(m_1, m_2)) \right) \geq 1 - \delta \right\} \geq 1 - \gamma$$

and

$$p \left\{ \sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left(D_{X^n(m_1, m_2)}^{(2)} W_2^{\otimes n}(X^n(m_1, m_2)) \right) \geq 1 - \delta \right\} \geq 1 - \gamma .$$

Thus,

$$\begin{aligned}
&p \left\{ \sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left(D_{X^n(m_1, m_2)}^{(1)} W_1^{\otimes n}(X^n(m_1, m_2)) \right) \geq 1 - \delta \text{ and} \right. \\
&\quad \left. \sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left(D_{X^n(m_1, m_2)}^{(2)} W_2^{\otimes n}(X^n(m_1, m_2)) \right) \geq 1 - \delta \right\} \\
&\geq 1 - 2\gamma .
\end{aligned}$$

If n is sufficiently large, with a positive probability, we can find a realization $x^n(m_1, m_2)$ of $X^n(m_1, m_2)$ such that

$$\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left(D_{x^n(m_1, m_2)}^{(1)} W_1^{\otimes n}(x^n(m_1, m_2)) \right) \geq 1 - \delta ,$$

and

$$\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left(D_{x^n(m_1, m_2)}^{(2)} W_2^{\otimes n}(x^n(m_1, m_2)) \right) \geq 1 - \delta .$$

Definition of the message sets:

Assume

$$\left| \left\{ m_2 \in M'_2 : \sum_{m_2 \in M'_2} \frac{1}{|M'_2|} \text{tr} \left(D_{x^n(m_1, m_2)}^{(1)} W_1^{\otimes n}(x^n(m_1, m_2)) \right) < 1 - 2\delta \right\} \right| > \frac{1}{2} |M'_2| .$$

We have in this case,

$$\sum_{m_1 \in M'_1} \sum_{m_2 \in M'_2} \frac{1}{|M'_1||M'_2|} \text{tr} \left(D_{x^n(m_1, m_2)}^{(1)} W_1^{\otimes n}(x^n(m_1, m_2)) \right) < 1 - \delta ,$$

but this is a contradiction to the result above.

Thus, there exists a set $M_2 \in M'_2$ such that $|M_2| = \lceil \frac{1}{2} |M'_2| \rceil$ and for every $m_2 \in M_2$ we have

$$\sum_{m_1 \in M'_1} \frac{1}{|M'_1|} \text{tr} \left(D_{x^n(m_1, m_2)}^{(1)} W_1^{\otimes n}(x^n(m_1, m_2)) \right) \geq 1 - 2\delta . \quad (24)$$

Similarly, there exists a set $M_1 \in M'_1$ such that $|M_1| = \lceil \frac{1}{2} |M'_1| \rceil$ and for every $m_1 \in M_1$ we have

$$\sum_{m_2 \in M'_2} \frac{1}{|M'_2|} \text{tr} \left(D_{x^n(m_1, m_2)}^{(2)} W_2^{\otimes n}(x^n(m_1, m_2)) \right) \geq 1 - 2\delta . \quad (25)$$

For every $(m_1, m_2) \in M_1 \times M_2$, we define

$$w((m_1, m_2)) := x^n(m_1, m_2) , \quad (26)$$

$$D_{m_2}^{(m_1)} := D_{x^n(m_1, m_2)}^{(1)} , \quad (27)$$

and

$$D_{m_1}^{(m_2)} := D_{x^n(m_1, m_2)}^{(2)} . \quad (28)$$

$\{D_{m_1}^{(m_2)} : m_1 \in M_1\}$ is less or equal to the partition of the identity for every $m_2 \in M_2$. $\{D_{m_2}^{(m_1)} : m_2 \in M_2\}$ is less or equal to the partition of the identity for every $m_1 \in M_1$.

Since node 1 already knows the message $m_2 \in M_2$, it chooses the corresponding decoding set

$$\left\{ D_m^{(m_2)} : m \in M_1 \right\}$$

to decode $m_1 \in M_1$. Since node 2 already knows the message $m_1 \in M_1$, it chooses the corresponding decoding set

$$\left\{ D_m^{(m_1)} : m \in M_2 \right\}$$

to decode $m_2 \in M_2$.

By (24) and (25), for every $m_2 \in M_2$ we have

$$\sum_{m_1 \in M_1} \frac{1}{|M_1|} \text{tr} \left(D_{m_1}^{(m_2)} W_1^{\otimes n} (x^n(m_1, m_2)) \right) \geq 1 - 4\delta, \quad (29)$$

and for every $m_1 \in M_1$ we have

$$\sum_{m_2 \in M_2} \frac{1}{|M_2|} \text{tr} \left(D_{m_2}^{(m_1)} W_2^{\otimes n} (x^n(m_1, m_2)) \right) \geq 1 - 4\delta. \quad (30)$$

Thus, for all sufficiently large $n \in \mathbb{N}$ any rate pairs satisfying

$$R_1 \leq \chi(P; \sigma^{Y_1}) - 2\epsilon - \frac{1}{n}$$

and

$$R_2 \leq \chi(P; \sigma^{Y_2}) - 2\epsilon - \frac{1}{n}$$

are achievable. \square

If we combine Lemma 1 and Theorem 1, we obtain

Corollary 1 *Let N be a two-phase bidirectional relaying quantum channel. Let H^{Y_1} be the Hilbert space whose unit vectors correspond to the pure states of node 1's quantum system, H^{Y_2} be the Hilbert space whose unit vectors correspond to the pure states of node 2's quantum system, and H^X be the Hilbert space whose unit vectors correspond to the pure states of the relay node's quantum system.*

We assume that the relay node's encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $X \subset H^X$.

We assume that node 1's encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $Y_1 \subset H^{Y_1}$.

We assume that node 2's encoding is restricted to transmitting an indexed finite set of orthogonal quantum states $Y_2 \subset H^{Y_2}$.

The classical-quantum capacity region of the two-phase bidirectional relaying quantum channel N with average error is the intersection of two rate regions, Region 1 and Region 2, which are defined as follows:

1: Region 1 is the set of all rate pairs (R_1, R_2) such that

$$R_2 \leq \chi(Q_1; \sigma^X), \quad (31)$$

$$R_1 \leq \chi(Q_2; \sigma^X), \quad (32)$$

and

$$R_2 + R_1 \leq \chi(Q_{1,2}; \sigma^X) \quad (33)$$

for any joint probability distribution $Q_{1,2}$ on $Y_1 \times Y_2$. Here Q_1 is the marginal probability distribution of $Q_{1,2}$ on Y_1 , Q_2 is the marginal probability distribution of $Q_{1,2}$ on Y_2 , and σ^X is the resulting quantum state at the outcome of the relay node.

2: Region 2 is the set of all rate pairs (R_1, R_2) such that

$$R_1 \leq \limsup_{n \rightarrow \infty} \frac{1}{n} \chi(P^n; \sigma^{Y_1 \otimes n}) \quad (34)$$

and

$$R_2 \leq \limsup_{n \rightarrow \infty} \frac{1}{n} \chi(P^n; \sigma^{Y_2 \otimes n}) \quad (35)$$

for all probability distribution P on X . Here, σ^{Y_1} is the resulting quantum state at the outcome of node 1, while σ^{Y_2} is the resulting quantum state at the outcome of node 2.

Remark 2 Note that the capacity region of a multiple-access channel with average errors is not equal to its capacity region with maximal errors. This is a well-known fact in the classical information theory (cf. [16] and [2]). We consider average errors, not maximal errors in Theorem 1 and Corollary 1, since we use Lemma 1, which considered average errors, for the multiple-access phase.

Remark 3 Without loss of generality, we assume that $\chi(P; \sigma^{Y_1}) \geq \chi(P; \sigma^{Y_2})$, i.e., W_2 , the channel which connects the relay node and node 2, has a lower capacity than W_1 in the broadcast phase. If $\chi(Q_2; \sigma^X) = \chi(P; \sigma^{Y_2})$, i.e., the capacities of W_2 in both directions are identical, then R_1 cannot exceed $\chi(P; \sigma^{Y_2})$ in the multiple-access phase. In this case, we may assume that in the broadcast phase the message sets $M_1 = \{1, \dots, |M_1|\}$ and $M_2 = \{1, \dots, |M_2|\}$, that the relay node sends to node 1 and node 2, satisfy $|M_1| \leq 2^{n\chi(P; \sigma^{Y_2}) - \epsilon}$ and $|M_2| \leq 2^{n\chi(P; \sigma^{Y_2}) - \epsilon}$ for a positive ϵ .

In this case, we have a very simple coding strategy for the broadcast phase. The common message set which the relay node sends to both node 1 and node 2 in the broadcast phase is a set $M' = \{1, \dots, |M'|\}$ which satisfies $|M'| = \lfloor 2^{n\chi(P; \sigma^{Y_2}) - \epsilon} \rfloor$.

We consider the case that the relay node wants to send $(m_1, m_2) \in M_1 \times M_2$, where node 1 shall detect m_1 , while node 2 shall detect m_2 . Then, the relay node sends $m_1 + m_2 \bmod |M'|$ as a common message to both node 1 and node 2. By the HSW Random Coding Theorem (cf. [41] and [21]) node 1 and node 2 can decode the common message if the size of the message set is less than $2^{n\chi(P; \sigma^{Y_2})}$.

Since node 1 already knows m_2 , it can obtain m_1 by simply subtracting m_2 from $m_1 + m_2$ modulo $|M'|$. Since node 2 already knows m_1 , it can obtain m_2 by subtracting m_1 from $m_1 + m_2$ modulo $|M'|$.

Acknowledgment

Support by the Bundesministerium für Bildung und Forschung (BMBF) via Grant 16BQ1050 and 16BQ1052 is gratefully acknowledged.

References

1. S. AbruZZo, S. Bratzik, N. K. Bernardes, H. Kampermann, P. van Loock, and D. Bruß, Quantum repeaters and quantum key distribution: analysis of secret key rates, *Phys. Rev. A*, Vol. 87, 052315, 2013.
2. R. Ahlswede, On two-way communication channels and a problem by Zarankiewicz, Sixth Prague Conf. on Inf. Th., Stat. Dec. Fct's and Rand. Proc., Publ. House Czechosl. Academy of Sc., Prague, pp. 23-37, 1973.
3. R. Ahlswede, Multi-way communication channels, Proceedings of 2nd International Symposium on Information Theory, Thakadsor, Armenian SSR, 1971, Akademiai Kiado, Budapest, pp. 23-52, 1973.
4. R. Ahlswede and V. Blinovsky, Classical capacity of arbitrarily classical-quantum varying channels, *IEEE Trans. Inform. Theory*, Vol. 53, No. 2, pp. 526-533, 2007.
5. M. Andersson, R. F. Schaefer (Wyrembelski), T. J. Oechtering, and M. Skoglund, Polar coding for bidirectional broadcast channels with common and confidential messages, *IEEE Journal on Selected Areas in Communications*, Vol. 31, No. 9, 1901-1908, 2013.
6. P. P. Bergmans, Random coding theorem for broadcast channels with degraded components, *IEEE Trans. Inf. Theory*, Vol. IT-19, No. 2, pp. 197-207, 1973.
7. I. Bjelaković, H. Boche, G. Janßen, and J. Nötzel, Arbitrarily varying and compound classical-quantum channels and a note on quantum zero-error capacities, *Information Theory, Combinatorics, and Search Theory*, in Memory of Rudolf Ahlswede, H. Aydinian, F. Cicalese, and C. Deppe eds., LNCS Vol. 7777, 247-283, [arXiv:1209.6325](#), 2012.
8. H. Boche, M. Cai, and C. Deppe, Classical-quantum arbitrarily varying wiretap channel - capacity formula with Ahlswede Dichotomy - resources, [arXiv:1307.8007](#), 2014.
9. H. Boche, N. Cai, and J. Nötzel, The classical-quantum channel with random state parameters known to the sender, [arXiv:1506.06479](#), 2015.
10. H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum repeaters for communication, [arXiv:quant-ph/9803056v1](#), 1998.
11. N. Cai, A. Winter, and R. W. Yeung, Quantum privacy and quantum wiretap channels, *Problems of Information Transmission*, Vol. 40, No. 4, 318-336, 2004.
12. T. M. Cover, Comments on broadcast channels, *IEEE Trans. Inf. Theory*, Vol. IT-44, pp. 2524-2530, 1998.
13. T. M. Cover and A. El Gamal, Capacity theorems for the relay channel, *IEEE Trans. Inf. Theory*, Vol. IT-25, No. 5, pp. 572-584, 1979.
14. I. Devetak, The private classical information capacity and quantum information capacity of a quantum channel, *IEEE Trans. Inform. Theory*, Vol. 51, No. 1, pp. 44-55, 2005.
15. T. T. Do, T. J. Oechtering, and M. Skoglund, Optimal transmission for the MIMO bidirectional broadcast channel in the wideband regime, *IEEE Trans. on Signal Processing*, Vol. 61, No. 20, pp. 5103-5116, 2013.
16. G. Dueck, Maximal error capacity regions are smaller than average error capacity regions for multi-user channels, *Probl. Contr. Inf. Theory*, Vol. 7, No. 1, pp. 11-19, 1978.
17. J. Eisert and M. M. Wolf, *Gaussian Quantum Channels*, *Quantum Information with Continuous Variables of Atoms and Light*, Imperial College Press, London, pp. 23-42, 2007.
18. A. El Gamal and E. Van der Meulen, A proof of Marton's coding theorem for the discrete memoryless broadcast channel, *IEEE Trans. Inf. Theory*, Vol. IT-27, pp. 120-122, 1981.

19. M. Hayashi and H. Nagaoka, General formulas for capacity of classical-quantum channels, *IEEE Trans. Inf. Theory*, Vol. 49, No. 7, pp. 1753-1768, 2003.
20. A. S. Holevo, Statistical problems in quantum physics, *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, ser. *Lecture Notes in Mathematics*, G. Maruyama and J. V. Prokhorov, Eds., Vol. 330, pp. 104-119, Springer-Verlag, Berlin, 1973.
21. A. S. Holevo, The capacity of the quantum channel with general signal states, *IEEE Trans. Inf. Theory*, Vol. 44, pp. 269-273, 1998.
22. S. Ishizaka and T. Hiroshima, Quantum teleportation scheme by selecting one of multiple output ports. *Phys. Rev. A*, Vol. 79, 042306, 2009.
23. B.C. Jacobs, T.B. Pittman, and J.D. Franson, Quantum relays and noise suppression using linear optics, *Phys. Rev. A*, Vol. 66, 052307, No. 5, 2002.
24. G. Kramer, M. Gastpar, and P. Gupta, Cooperative strategies and capacity for relay networks, *IEEE Trans. Inf. Theory*, Vol. 51, No. 9, pp. 3037-3063, 2005.
25. H. Liao, Multiple access channels, Ph.D. dissertation, Department of Electrical Engineering, University of Hawaii, Honolulu, 1972.
26. K. Marton, A coding theorem for the discrete memoryless broadcast channel, *IEEE Trans. Inf. Theory*, Vol. IT-25, pp. 306-311, 1979.
27. T. J. Oechtering and H. Boche, Stability region of an optimized bidirectional regenerative half-duplex relaying protocol. *IEEE Trans. on Communications* Vol. 56, No. 9, pp. 1519-1529, 2008.
28. T. J. Oechtering and H. Boche, Bidirectional regenerative half-duplex relaying using relay selection, *IEEE Transactions on Wireless Communications*, Vol. 7, No. 5, pp. 1879-1888, 2008.
29. T. J. Oechtering, H. Boche, Optimal time-division for bidirectional relaying using superposition encoding, *IEEE Communications Letters*, Vol. 12, No. 4, 265-267, 2008.
30. T. J. Oechtering, E. A. Jorswieck, R. F. Schaefer (Wyrembelski), and H. Boche, On the optimal transmit strategy for the MIMO bidirectional broadcast channel. *IEEE Trans.*
31. T. J. Oechtering and M. Skoglund, Bidirectional broadcast channel with random states noncausally known at the encoder, *IEEE Trans. Inf. Theory*, Vol. 59, No. 1, pp. 64-75, 2013.
32. T. J. Oechtering, R. F. Schaefer (Wyrembelski), and H. Boche, Multiantenna bidirectional broadcast channels - optimal transmit strategies *IEEE Trans. on Signal Processing*, Vol. 57, No. 5, pp. 1948-1958, 2009. *on Communications*, Vol. 57, No. 12, pp. 3817-3826, 2009.
33. T. J. Oechtering, C. Schnurr, I. Bjelaković, and H. Boche, Broadcast capacity region of two-phase bidirectional relaying, *IEEE Trans. Inf. Theory*, Vol. 54, No. 1, pp. 454-458, 2008.
34. T. Ogawa and H. Nagaoka, Making good codes for classical-quantum channel coding via quantum hypothesis testing, *IEEE Trans. Inform. Theory*, Vol. 53, No. 6, 2261-2266, 2007.
35. I. Savov and M. Wilde, Classical codes for quantum broadcast channels, *Proceedings of ISIT 2012*, pp. 721-725, 2012.
36. I. Savov, M. Wilde, and M. Vu, Partial decode-forward for quantum relay channels, *Proceedings of ISIT 2012*, pp. 731-735, 2012.
37. R. F. Schaefer (Wyrembelski), T. J. Oechtering, and H. Boche, MIMO Gaussian bidirectional broadcast channels with common messages, *IEEE Trans. on Wireless Communications*, Vol. 10, No. 9, pp. 2950-2959, 2011.
38. R. F. Schaefer (Wyrembelski), I. Bjelaković, T. J. Oechtering, and H. Boche, Optimal coding strategies for bidirectional broadcast channels under channel uncertainty. *IEEE Trans. on Communications*, Vol. 58, No. 10, pp. 2984-2994, 2010.
39. R. F. Schaefer (Wyrembelski), M. Wiese, and H. Boche, Strong secrecy in bidirectional broadcast channels with confidential messages, *IEEE Trans. on Information Forensics and Security*, Vol. 8, No. 2, pp. 324-334, 2013.
40. B. Schumacher and M. A. Nielsen, Quantum data processing and error correction, *Phys. Rev. A*, Vol. 54, 2629, 1996.
41. B. Schumacher and M. D. Westmoreland, Sending classical information via noisy quantum channels, *Phys. Rev. A*, Vol. 56, pp. 131-138, 1997.

-
42. M. Wilde, Quantum Information Theory, Cambridge University Press, 2013.
 43. M. Wilde and S. Guha, Polar codes for classical-quantum channels, *IEEE Trans. Inf. Theory*, Vol. 59, No. 2, pp. 1175-1187, 2013.
 44. A. Winter, Coding theorem and strong converse for quantum channels, *IEEE Trans. Inf. Theory*, Vol. 45, No. 7, pp. 2481-2485, 1999.
 45. A. Winter, The capacity of the quantum multiple-access channel, *IEEE Trans. Inf. Theory*, Vol. 47, No. 7, pp. 3059-3065, 2001.
 46. J. Yard, P. Hayden, and I. Devetak, Capacity theorems for quantum multiple access channels — classical-quantum and quantum-quantum capacity regions, *IEEE Trans. Inf. Theory*, Vol. 54, No. 7, pp. 3091-3113, 2008.